Stockholms stad

Bilaga 9

GDPR årsrapport

År 2025

Enskede-Årsta-Vantörs stadsdelsnämnd

GDPR årsrapport
2025

Dnr: EÅV 2025/948
Utgivningsdatum: 2026-02-20
Kontaktperson: Nicole Melkie

Sammanfattning

GDPR, eller dataskyddsförordningen, syftar till att skydda individers grundläggande rättigheter och friheter, med särskilt fokus på rätten till skydd av personuppgifter. I Stockholms stad är varje nämnd och styrelse ansvarig för personuppgiftsbehandlingar som sker i den egna verksamheten. Ett dataskyddsombud har i uppdrag att oberoende granska verksamhetens efterlevnad av dataskyddsförordningen. I denna rapport redovisar dataskyddsombudet årets granskning av Enskede-Årsta-Vantörs stadsdelsnämnds dataskyddsarbete samt lämnar rekommendationer på åtgärder för att ytterligare stärka dataskyddet.

2025 har präglats av den omfattande och allvarliga personuppgiftsincident som inträffade när Miljödata utsattes för en dataläcka orsakad av en antagonistisk aktör. Incidenten påverkade ett stort antal aktörer, inklusive flera offentliga verksamheter, och kom att kräva ett intensivt och samordnat arbete inom staden. Hanteringen av händelsen underströk på ett tydligt sätt betydelsen av en stark informationssäkerhetskultur och hur centralt det är att skydda personuppgifter i både ordinarie verksamhet och vid extraordinära händelser.

Sammantaget visar året på behovet av fortsatt prioritering av informationssäkerhets- och dataskyddsarbete, både operativt och strategiskt, samt vikten av att säkerställa tillräckliga resurser för dataskyddsombudets uppdrag.

De tre största riskerna enligt dataskyddsombudets bedömning

Fråga/kontroll	Risk	Rekommenderad åtgärd/åtgärder
Brist vid information till berörda personer vid personuppgiftsincident		Rekommenderad åtgärd är att säkerställa att berörda personer informeras vid varje personuppgiftsincident som innebär hög risk. Det är viktigare att den berörda individen får information än att en anmälan görs till Integritetsskyddsmyndigheten (IMY).
Brist vid tröskelanalys och konsekvensbedömningar		Rekommenderad åtgärd är att leda och tilldela resurser till verksamheter och stödfunktioner så att informationsklassningar, riskanalyser och konsekvensbedömningar genomförs, samt säkerställa att resultaten omsätts i praktiken.
Bristande systematik och styrning		Dataskydd behöver vara en naturligt integrerad del av det dagliga arbetet för att personuppgiftsansvarig (PUA) ska uppfylla kraven i lagstiftningen och stadens riktlinjer. En rekommenderad åtgärd är att stärka styrningen inom området för att möjliggöra kontinuerlig uppföljning av linjeansvaret för dataskyddsfrågorna, vilket i sin tur bidrar till ökad systematik och bättre integration i verksamheten.

Innehållsförteckning

Inledning

GDPR, eller dataskyddsförordningen, syftar till att skydda individers grundläggande rättigheter och friheter, med särskilt fokus på rätten till skydd av personuppgifter. Dataskyddsreglerna (*kallas GDPR fortsättningsvis*) sätter tydliga ramar för hur personuppgifter får behandlas för att minimera risken för skada och säkerställa att hanteringen sker ansvarsfullt och rättvist. GDPR har sin grund i de mänskliga rättigheterna, där varje individ har rätt till respekt för sitt privat- och familjeliv samt skydd av sina personuppgifter.

I Stockholms stad är varje nämnd och styrelse ansvarig för personuppgiftsbehandlingar som sker i den egna verksamheten.

Dataskyddsombudets uppgift

Varje personuppgiftsansvarig (nämnd eller styrelse) ska utse ett dataskyddsombud. Dataskyddsombudets uppgifter framgår direkt av lagstiftningen. Ombudets roll är att kontrollera att GDPR följs inom organisationen. Det innebär bland annat att ge råd, rekommendationer och informera om frågor som rör behandlingar av personuppgifter. Dataskyddsombudet har även i uppdrag att oberoende granska verksamheternas arbete med dataskyddsfrågor för att säkerställa att dataskyddslagstiftningen efterlevs. Dataskyddsombudet ska rapportera direkt till högsta förvaltnings-/bolagsnivå. I Stockholms stad innebär det att dataskyddsombudet rapporterar till nämnder och styrelser.

Dataskyddsombudet lämnar årligen en rapport om verksamhetens dataskyddsarbete till varje nämnd och styrelse. Genom rapporten kan nämnd och styrelse ta emot de råd och rekommendationer som dataskyddsombudet lämnar. Årsrapporten syftar till att nämnd/styrelse ska kunna fatta beslut om prioriteringar, resurser och initiativ framåt. Årsrapporten är ett medel för nämnds/styrelsens uppföljning och styrning av verksamhetens systematiska integritets- och dataskyddsarbete.

Granskning av dataskyddsarbetet 2025

Kontroll av obligatoriska områden

Dataskyddsombudet har granskat verksamhetens dataskyddsarbete utifrån sex obligatoriska områden. De sex områdena har identifierats genom en analys av kraven i GDPR om hur verksamheter bör arbeta systematiskt med dataskydd. Varje område innehåller ett antal kontrollfrågor som ger en bild av verksamhetens dataskyddsarbete. Dessa områden överensstämmer med de delar som enligt IMY utgör grunden för en verksamhets systematiska och rättssäkra hantering av personuppgifter.

I rapporten används en riskmodell med fyra nivåer av risk. Modellen hjälper dataskyddsombudet att visa vilken bedömning hen gör av verksamhetens dataskyddsrisker utifrån de iakttagelser som gjorts i granskningen.

Risknivå	Beskrivning
Hög risk 	Iakttagelsen avser en brist som kan leda till betydande risker för de registrerades rättigheter och friheter. Bristen kräver omgående åtgärd och korrigering.
Medelhög risk 	Iakttagelsen avser en brist som kan leda till risker för de registrerades rättigheter och friheter. Bristen bör åtgärdas skyndsamt, men kräver inte omedelbar korrigering.
Låg risk 	Iakttagelsen avser en brist som kan leda till mindre risker för de registrerades rättigheter och friheter. Bristen bör åtgärdas, men kräver inte omedelbar korrigering.
Inget att anmärka 	Dataskyddsombudet har inga brister att rapportera avseende denna del.

Notera att risken för att tilldelas en sanktion vid tillsyn är större ju högre risken är.

Resultatsammanställning och centrala iakttagelser inom dataskyddsarbetet

I detta avsnitt presenteras en sammanställning av den bedömda risknivån för verksamhetens dataskyddsarbete, grundat på kontrollfrågorna inom de sex obligatoriska områdena. Vidare redovisas dataskyddsombudets centrala iakttagelser, inklusive områden där verksamheten uppvisar goda resultat och bör upprätthålla sitt arbete, samt identifierade brister som kan utgöra dataskyddsrisker. Avsnittet innehåller även dataskyddsombudets rekommenderade åtgärder för att hantera dessa risker och stärka dataskyddsarbetet.

En fullständig redovisning av dataskyddsombudets underlag och resultat från granskningen av de sex obligatoriska områdena finns att läsa i bilaga 1. Bilagan innehåller även en beskrivning av syftet och bakgrunden för varje område.

Register över personuppgiftsbehandlingar

Sammanfattning

Dataskyddsombudets samlade bedömning är att stadsdelsförvaltningen i stort har genomfört de nödvändiga uppdateringarna av registerförteckningen över personuppgiftsbehandlingar. Samtliga avdelningar har arbetat aktivt med att se över och revidera sina registreringar, och årets uppföljning visar att majoriteten av de uppdateringar som krävs enligt rutinen har genomförts.

Vid genomgången har dataskyddsombudet dock uppmärksammat att risknivå i många fall saknas i registreringarna. Eftersom riskklassificeringen är en central del av arbetet med att bedöma och prioritera lämpliga skyddsåtgärder innebär avsaknaden av denna uppgift att det blir svårt att skapa en tydlig överblick över vilka behandlingar som kan innebära högre risker. Detta försvårar också möjligheten att arbeta enligt dataskyddsförordningens riskbaserade ansats.

Sammanfattningsvis bedöms registerförteckningen vara uppdaterad i huvudsak, men komplettering av risknivåer är nödvändig för att säkerställa en heltäckande och ändamålsenlig dokumentation.

Bedömning av risknivå och rekommendationer från dataskyddsombudet

Fråga/kontroll	Risk	Rekommendationer
Antal behandlingar som är registrerade?		*550. Verksamheterna har sett över vilka behandlingar som finns på verksamheterna.*
Har verksamheten ändamålsenliga rutiner för att registrera nya/förändrade behandlingar?		*Ja. Verksamheterna följer stadsdelsnämndens rutiner för nya/förändrade behandlingar.*

Registreras/uppdateras behandlingar i den omfattning som krävs för att registret ska innehålla de behandlingar som personuppgiftsansvarig utför?		*Ja. Verksamheterna uppdaterar sina behandlingar årligen. Dock försvinner risknivåerna vid uppdatering och i en del fall glöms det bort att de behöver läggas till igen.*
Har de uppgifter som är obligatoriska enligt artikel 30 besvarats kopplat till de registrerade behandlingarna?		*Ja.*

Säkerhet i samband med behandlingen

Sammanfattning

Stadsdelsförvaltningen har en förteckning över genomförda informationsklassningar som administreras och samordnas av informationssäkerhetssamordnaren. Förteckningen ger en överblick över vilka informationstillgångar och system som har informationsklassats, när klassningen genomfördes samt vilka skyddsnivåer som gäller för respektive tillgång.

Informationssäkerhetssamordnaren arbetar aktivt med att uppdatera befintliga klassningar för att säkerställa att de fortsatt speglar verksamhetens aktuella behov och risker. Parallellt pågår arbetet med att informationsklassa nya system allt eftersom de införs eller identifieras. Detta bidrar till att stadsdelsförvaltningen successivt stärker sitt systematiska arbete med informationssäkerhet och säkerställer att skyddsåtgärderna är anpassade efter den risknivå som olika informationstillgångar innebär.

Bedömning av risknivå och rekommendationer från dataskyddsombudet

Fråga/kontroll	Risk	Rekommendationer
Efter ett antal stickprov på genomförda informationsklassningar, bedömer DSO att resultatet i genomförda informationsklassningar i tillräcklig utsträckning tar hänsyn till olika kategorier av personuppgifter?		*Ja.*

Avseende de styrande dokument och rutiner om dataskydd (som finns skriftligt), bedömer DSO att det finns tillräckligt mycket reglerat och tillräckligt stöd?		*Ja. Styrande dokument och rutiner ses över årligen och uppdateras vid behov.*
Avseende de skriftligt styrande dokument och rutiner som finns, bedömer DSO att de är tillräckligt implementerade och kända?		*Ja. Alla rutiner som avser GDPR är publicerade på intranätet..*

Konsekvensbedömning avseende dataskydd

Sammanfattning

Dataskyddsombudet bedömer att konsekvensbedömningar (DPIA) ännu inte har genomförts för alla behandlingar som potentiellt kan innebära hög risk för de registrerades rättigheter och friheter. Även om stadsdelsförvaltningen har en välstrukturerad och omfattande registerförteckning saknas det ofta uppgifter om risknivå för de registrerade behandlingarna.

Denna brist gör det svårt att identifiera vilka behandlingar som faktiskt bör konsekvensbedömas och innebär att det kan saknas DPIA:er för vissa högriskbehandlingar. Dataskyddsombudet kan därmed konstatera att konsekvensbedömningar saknas, men det är i nuläget inte möjligt att fastställa omfattningen eller exakt vilka behandlingar som borde ha omfattats.

Sammanfattningsvis behöver riskklassificeringen i registerförteckningen kompletteras för att möjliggöra en mer träffsäker och systematisk bedömning av när DPIA krävs och för att stärka det riskbaserade arbetet inom stadsdelsförvaltningen.

Bedömning av risknivå och rekommendationer från dataskyddsombudet

Fråga/kontroll	Risk	Rekommendationer
Finns det ändamålsenliga rutiner för att vid nya/förändrade personuppgiftsbehandlingar genomföra tröskelanalys?		*Ja, stadsdelsnämnden har rutiner som verksamheterna följer.*
Genomförs tröskelanalyser vid nya/förändrade personuppgiftsbehandlingar?		*Delvis. Tröskelanalyser är ett arbete som behöver fortsätta och utvecklas. Det finns behandlingar som inte har tröskelanalys.*

Finns det en ändamålsenlig mall samt rutiner för genomförande av konsekvensbedömning avseende dataskydd?		*Ja.*
Genomförs konsekvensbedömning avseende dataskydd i de fall det krävs?		*Delvis. Arbetet med konsekvensbedömningar behöver utvecklas och göras vid varje högriskbehandling.*
Har personuppgiftsansvarig identifierat samtliga personuppgiftsbehandlingar som kräver att en konsekvensbedömning avseende dataskydd görs samt genomfört detta?		*Delvis. Det är ett pågående arbete.*

Den registrerades rättigheter

Sammanfattning

Dataskyddsombudet bedömer att stadsdelsförvaltningen har goda förutsättningar för att hantera registrerades rättigheter inom den tidsfrist som dataskyddsförordningen anger. Stadsdelsförvaltningen har en etablerad och tydligt dokumenterad rutin som beskriver hur begäranden från registrerade ska tas emot, bedömas och besvaras. Rutinen säkerställer att handläggningen sker på ett strukturerat och rättssäkert sätt.

Som en del av uppföljningen för dataskyddsarbetet för dataskyddsombudet ett register över samtliga inkomna begäranden. Detta register möjliggör löpande uppföljning av hur många ärenden som inkommit, vilken typ av rättigheter som hänvisats till samt om svar lämnats inom föreskriven tid. Genom denna struktur finns goda förutsättningar att upprätthålla en enhetlig hantering och att snabbt identifiera eventuella brister eller behov av förbättringar.

Sammanfattningsvis visar årets granskning att stadsdelsförvaltningen har en välfungerande process för att hantera registrerades rättigheter.

Bedömning av risknivå och rekommendationer från dataskyddsombudet

Fråga/kontroll	Risk	Rekommendationer
Finns det ändamålsenliga mallar samt rutiner för besvarande av begäran från den registrerade?		*Ja. Stadsdelsnämnden har mallar samt rutiner på hur begäran ska ske.*
Hur många begäranden (om registerutdrag, begränsning, radering etc.) har under året inkommit från de registrerade?		*5.*
Hur många av de inkomna begärandena har besvarats av verksamheten inom en månad?		*Alla utom en. Denna inkom genom dom, och tog någon dag extra att besvara.*
Baserat på ett antal stickprov genomförda av dataskyddsombudet, uppfyller svaren till de registrerade lagkraven?		*Ja. Stadsdelsnämnden har mallar att följa på hur nämnden ska svara vid begäran.*

Personuppgiftsincidenter

Sammanfattning

Dataskyddsombudet har granskat stadsdelsförvaltningens register över rapporterade personuppgiftsincidenter. Genomgången visar att ungefär 60 procent av incidenterna har rapporterats in inom föreskriven tid, det vill säga inom 72 timmar från det att incidenten upptäcktes. I de återstående fallen har fördröjningen främst berott på att verksamheterna saknat tillräcklig kunskap om hur de ska agera när en incident inträffar och därför inte rapporterat vidare händelsen i tid.

För att stärka arbetet inom området har stadsdelsförvaltningen under året uppdaterat rutinen för hantering av personuppgiftsincidenter. Den reviderade rutinen tydliggör ansvarsfördelningen mellan medarbetare, närmaste chef och dataskyddsombudet, vilket syftar till att skapa en mer strukturerad och rättssäker incidenthantering. Genom att klargöra roller och processer förväntas rutinen bidra till snabbare rapportering och bättre efterlevnad av dataskyddsförordningens krav.

Sammanfattningsvis visar årets granskning att det finns en fungerande struktur för incidenthantering, men att kunskapshöjande insatser och fortsatt förankring av rutinen är nödvändiga för att öka rapporteringen inom den lagstadgade tidsfristen.

Bedömning av risknivå och rekommendationer från dataskyddsombudet

Fråga/kontroll	Risk	Rekommendationer
Hur säkerställs det att samtliga medarbetare har den kunskap som behövs för att veta hur denne ska agera vid en personuppgiftsincident?		*Rutiner och information finns på intranätet. Chefer ansvarar för att informera sina medarbetare.*
Finns det ändamålsenliga rutiner för att hantera händelser som kan utgöra potentiella personuppgiftsincidenter? Följs dessa?		*Ja.*
Hur många personuppgiftsincidenter har dokumenterats under året?		*Totalt 17 stycken.*
Hur många personuppgiftsincidenter har anmälts till IMY under året?		*13 stycken.*

Överföring till tredje land

Sammanfattning

Vid dataskyddsombudets genomgång av stadsdelsförvaltningens registerförteckning, personuppgiftsbiträdesavtal, genomförda konsekvensbedömningar samt påbörjade och avslutade informationsklassningar kan det konstateras att stadsdelsförvaltningen har identifierat och dokumenterat förekomsten av tredjelandsöverföring.

Den tredjelandsöverföring som har identifierats är kopplad till användningen av Zoom X, ett system som är upphandlat på central nivå inom staden. I och med den centrala upphandlingen hanteras bedömningar av överföringen, tillämpliga överföringsmekanismer samt eventuella kompletterande skyddsåtgärder av stadens centrala funktioner. Stadsdelsförvaltningen följer därmed de riktlinjer, riskbedömningar och säkerhetsåtgärder som fastställts inom ramen för det centrala avtalet.

Under slutet av året har dock Zoom X ersatts av tjänsten Nordic for Zoom, vilket innebär en säkrare lösning där servrarna är placerade i Sverige. Denna lösning bedöms inte innebära någon tredjelandsöverföring, vilket på sikt minskar behovet av särskilda skyddsåtgärder kopplade till överföring av personuppgifter utanför EU/EES.

Sammanfattningsvis visar granskningen att stadsdelsförvaltningen på ett korrekt och strukturerat sätt har dokumenterat den tredjelandsöverföring som förekommit samt att överföringen varit kopplad till ett centralt upphandlat system där ansvaret för vidare bedömningar och åtgärder ligger på stadsnivå.

Bedömning av risknivå och rekommendationer från dataskyddsombudet

Fråga/kontroll	Risk	Rekommendationer
Har personuppgiftsansvarig identifierat de tredjelandsöverföringar som utförs?		*En personuppgiftsbehandling har identifierats.*
Tillämpar personuppgiftsansvarig ett överföringsverktyg på de tredjelandsöverföringar som utförs?		*För den identifierade personuppgiftsbehandlingen gäller standardavtalsklausuler.*
Har personuppgiftsansvarig gjort en nödvändig bedömning, ”Transfer Impact Assessment” (TIA), avseende tredjelandsöverföringar?		*Delvis. Det finns ingen TIA som stadsdelsförvaltningen har fått ta del av gällande Nordic for Zoom.*

Bilagor

Bilaga 1: Detaljerad redovisning av dataskyddsombudets granskning

Bilaga 2: Andra genomförda granskningar och omvärldsbevakning

Bilaga 1 - Detaljerad redovisning av dataskyddsombudets granskning

Denna bilaga innehåller en beskrivning av syftet med respektive obligatoriskt område samt en mer detaljerad redovisning av dataskyddsombudets granskningar och slutsatser. Här framgår vilka iakttagelser som gjorts och vilken information som samlats in under granskningsarbetet av de sex obligatoriska rapporteringsområdena. För varje område redovisas de underlag som har använts, de iakttagelser som har gjorts samt hur dessa har utgjort grunden för dataskyddsombudets riskbedömning och rekommenderade åtgärder.

1. Register över personuppgiftsbehandlingar

Bakgrund och syfte

I GDPR framkommer det att personuppgiftsansvariga (och personuppgiftsbiträden) ska föra ett register över sina personuppgiftsbehandlingar. Registret brukar benämnas ”behandlingsregister” eller ”registerförteckning”. Registret ska finnas tillgängligt i elektronisk form och ska omfatta samtliga personuppgiftsbehandlingar som personuppgiftsansvarig utför. Det ska hållas uppdaterat vilket innebär att det ska uppdateras vid nya eller förändrade personuppgiftsbehandlingar.

Syftet med detta rapporteringsområde är att rapportera om verksamheten har ändamålsenliga rutiner som möjliggör att nya/förändrade personuppgiftsbehandlingar registreras, huruvida personuppgiftsbehandlingar registreras/uppdateras såsom det krävs samt huruvida de uppgifter som är obligatoriska har besvarats kopplat till de registrerade personuppgiftsbehandlingarna.

Kontroller och iakttagelser gjord av dataskyddsombudet

Antal behandlingar som är registrerade?

550 stycken

Har verksamheten ändamålsenliga rutiner som möjliggör att nya/förändrade behandlingar registreras?

Dataskyddsombudet bedömer att stadsdelsförvaltningen har ändamålsenliga och välfungerande rutiner för att säkerställa att nya eller förändrade personuppgiftsbehandlingar registreras korrekt. Under året skickar dataskyddsombudet ut återkommande påminnelser till verksamheterna om att regelbundet gå igenom sina registreringar, i syfte att säkerställa att informationen är aktuell, fullständig och överensstämmer med gällande behandlingar.

Enligt gällande rutin har varje avdelningschef det yttersta ansvaret för att en systematisk inventering av personuppgiftsbehandlingar genomförs inom den egna avdelningen. Denna inventering ska göras årligen under det första kvartalet. Utifrån resultatet av inventeringen ska verksamheterna därefter uppdatera sina register i Draftit, så att eventuella nya behandlingar förs in och befintliga uppgifter justeras vid förändringar. Dessa moment syftar till att säkerställa en korrekt och uppdaterad registerföring över samtliga behandlingar inom stadsdelsförvaltningen.

Registreras/uppdateras behandlingar i den omfattning som krävs för att registret ska innehålla de behandlingar som personuppgiftsansvarig utför?

Ja. Enligt stadsdelsförvaltningens fastställda rutin ska samtliga personuppgiftsbehandlingar ses över och uppdateras årligen under det första kvartalet. I samband med denna genomgång kontrollerar verksamheterna om befintliga registreringar fortfarande är aktuella, om någon information behöver justeras eller om behandlingar har tillkommit eller upphört. Syftet är att säkerställa att registret alltid återspeglar de behandlingar som den personuppgiftsansvarige faktiskt utför och att informationen hålls korrekt, komplett och uppdaterad.

Har de uppgifter som är obligatoriska enligt artikel 30 besvarats kopplat till de registrerade behandlingarna?

Ja. Dataskyddsombudet genomför regelbundna stickprovskontroller av registrerade behandlingar under året. Vid dessa granskningar har dataskyddsombudet kunnat konstatera att samtliga obligatoriska uppgifter enligt artikel 30 i dataskyddsförordningen har besvarats för de behandlingar som kontrollerats. Detta innebär att registren innehåller de uppgifter som krävs för att uppfylla förordningens krav på dokumentation av personuppgiftsbehandlingar.

Dataskyddsombudets jämförelse med föregående års resultat

Dataskyddsombudet bedömer att registreringen av behandlingar fortsatt håller en god kvalitet. Under 2024 fanns totalt 575 registrerade behandlingar. Inför årets uppföljning har antalet minskat till 550. Minskningen beror dock inte på brister i registerföringen, utan är en följd av den omorganisation som genomförts inom stadsdelsförvaltningen.

I samband med omorganisationen har flera verksamheter och avdelningar slagits samman. Detta medförde att vissa behandlingar tidigare fanns registrerade flera gånger, en registrering per verksamhet, trots att behandlingen i praktiken var densamma. Under året har registreringarna därför konsoliderats, så att en avdelning nu har en gemensam och samlad registrering för behandlingar som används av flera verksamheter inom avdelningen.

Det minskade antalet registreringar är således ett resultat av en ökad tydlighet och samordning, och inte av att behandlingar saknas i registret. Dataskyddsombudets bedömning är att förändringen har lett till ett mer överskådligt och korrekt register.

Skiljer sig resultatet åt från föregående år och hur i så fall?

Resultatet går inte att jämföra fullt ut med föregående år eftersom föregående års årsrapport hade en annan struktur och upplägg. Trots skillnaderna i utformning visar årets genomgång i princip samma övergripande resultat som tidigare. Dataskyddsombudet bedömer därför att nivån på registerföringen och efterlevnaden av rutinerna är oförändrat god, även om rapporternas utformning gör en exakt jämförelse svår.

Dataskyddsombudets bedömning samt rekommendationer

Dataskyddsombudets samlade bedömning är att merparten av de nödvändiga uppdateringarna i registerförteckningen har genomförts och att arbetet med registerföring överlag fungerar väl.

Flera enheter har kommit långt i sitt arbete och kan lyftas som goda exempel på hur rutinerna bör följas och dokumentationen hållas aktuell.

En genomgång av hela registerförteckningen visar dock att det i majoriteten av behandlingarna saknas angiven risknivå. Avsaknaden av riskklassificering försvårar överblicken av vilka behandlingar som medför högre risker och därmed vilka skyddsåtgärder som bör prioriteras. Detta begränsar möjligheten att arbeta systematiskt med riskbaserat dataskydd.

Mot bakgrund av detta rekommenderar dataskyddsombudet att stadsdelsnämnden ger avdelningscheferna på samtliga avdelningar i uppdrag att se över och komplettera sina registreringar i Draftit med korrekt risknivå för respektive behandling. Vidare föreslår dataskyddsombudet att nämnden uppdrar åt dataskyddsombudet att följa upp att uppdateringarna genomförts samt att redovisa resultatet i årsrapporten för 2026.

2. Säkerhet i samband med behandlingen

Bakgrund och syfte

Personuppgiftsansvarig ska se till att personuppgifter skyddas med lämpliga säkerhetsåtgärder, detta för att till exempel undvika att obehöriga får tillgång till uppgifterna eller att uppgifterna förloras.

Personuppgiftsansvarig behöver bedöma vilka tekniska- och organisatoriska säkerhetsåtgärder som ska vidtas för de behandlingar som utförs. Till tekniska säkerhetsåtgärder räknas till exempel kryptering, pseudonymisering och säkerhetskopiering. Organisatoriska säkerhetsåtgärder avser till exempel interna riktlinjer och rutiner.

För att skapa förutsättningar för att skydda information (inklusive personuppgifter) med rätt slags skydd ska verksamheten informationsklassa sin information. Stadens riktlinjer för informationssäkerhet föreskriver att alla stadens informationstillgångar ska vara klassade med stöd av SKR:s verktyg KLASSA. Ansvaret för att informationsklassning genomförs ligger på den del av verksamheten som är informationsägare. Genom riskanalyser identifierar informationsägaren risker och väljer åtgärder för att minska riskerna. Risker i samband med personuppgiftsbehandling är en typ av risk som informationsägaren behöver omhänderta i riskanalyser.

Att det finns skriftliga, beslutade och kommunicerade styrdokument samt kända rutiner medför att medarbetarna vet hur de ska agera avseende frågor som rör dataskydd. Den personuppgiftsansvariga måste kunna *visa* hur GDPR efterlevs och styrdokument och rutiner är en viktig del i detta.

Syftet med detta rapporteringsområde är därmed att rapportera huruvida dataskyddsombudet bedömer att det tas hänsyn till risker för den registrerade och om dessa beaktas i tillräcklig mån i genomförda informationsklassningar och riskanalyser. Vidare bedömer dataskyddsombudet huruvida det finns tillräckligt mycket reglerat om dataskydd i styrdokument och rutiner samt om dessa är tillräckligt implementerade och kända.

Kontroller och iakttagelser gjord av dataskyddsombudet

Efter ett antal stickprov på genomförda informationsklassningar, bedömer dataskyddsombudet att resultatet i genomförda informationsklassningar i tillräcklig utsträckning tar hänsyn till olika kategorier av personuppgifter?

Ja. Efter att ha genomfört ett antal stickprov på de informationsklassningar som har genomförts bedömer dataskyddsombudet att klassningarna i tillräcklig utsträckning tar hänsyn till de olika kategorier av personuppgifter som behandlas. I stickproven framgår att verksamheterna beaktar såväl vanliga personuppgifter som särskilda kategorier av personuppgifter samt att risknivåer och skyddsvärde generellt bedöms på ett sätt som motsvarar de krav som ställs i informationssäkerhetsarbetet. Detta innebär att informationsklassningarna överlag ger en rimlig grund för att fastställa lämpliga skyddsåtgärder.

Avseende de skriftligt styrande dokument och rutiner som finns, bedömer dataskyddsombudet att det finns tillräckligt mycket reglerat och tillräckligt stöd?

Ja. Dataskyddsombudet bedömer att de skriftligt styrande dokument och rutiner som finns sammantaget ger ett tillräckligt stöd för verksamheternas arbete med dataskydd. Stadsdelsförvaltningen har etablerade processer för att regelbundet se över och uppdatera dessa dokument, vilket sker minst en gång per år. De reviderade rutinerna publiceras därefter på stadsdelsförvaltningens intranät så att de är lätt tillgängliga för samtliga medarbetare.

Denna återkommande översyn bidrar till att säkerställa att styrdokumenten är aktuella, ändamålsenliga och i linje med gällande regelverk, vilket i sin tur skapar goda förutsättningar för en enhetlig och korrekt tillämpning i verksamheten.

Avseende de skriftligt styrande dokument och rutiner som finns, bedömer dataskyddsombudet att de är tillräckligt implementerade och kända?

Ja. Dataskyddsombudet bedömer att de skriftligt styrande dokumenten och rutinerna i huvudsak är tillräckligt implementerade och kända i organisationen. Samtliga dokument finns publicerade på stadsdelsförvaltningens intranät, där både medarbetare och chefer har enkel åtkomst till dem.

Genom att rutinerna finns samlade på en gemensam plattform skapas goda förutsättningar för att de ska vara kända och kunna tillämpas i det dagliga arbetet. Cheferna har dessutom en viktig roll i att sprida informationen och säkerställa att medarbetarna känner till och följer de aktuella riktlinjerna. Sammantaget bedömer dataskyddsombudet därför att implementeringen är tillräcklig, även om kontinuerlig information och påminnelser fortsatt är viktiga för att upprätthålla kunskapen över tid.

Dataskyddsombudets jämförelse med föregående års resultat

Skiljer sig resultatet åt från föregående år och hur i så fall?

Stadsdelsförvaltningen har en samlad förteckning över informationsklassningar som administreras av informationssäkerhetssamordnaren. Förteckningen ger en överblick över vilka informationstillgångar som innehåller personuppgifter och därmed omfattas av dataskyddsförordningen, samt när dessa senast har informationsklassats.

Av förteckningen framgår att det i dagsläget finns totalt 115 informationstillgångar som innehåller personuppgifter. Av dessa har 94 informationstillgångar informationsklassats, varav 61 är uppdaterade klassningar. Jämfört med föregående år har det totala antalet informationstillgångar minskat från 125 till 115. Minskningen beror på en genomförd översyn av samtliga system för att identifiera vilka som fortfarande är aktiva. I samband med denna genomgång har flera system avregistrerats, främst sådana som varit kopplade till tidsbegränsade projekt eller som ersatts av nyupphandlade system.

Samtidigt visar jämförelsen med föregående år att arbetet med informationsklassning har förstärkts avsevärt. Föregående år hade 77 av 125 informationstillgångar informationsklassats, varav endast 24 klassningar var uppdaterade. Årets resultat visar således att ett mer omfattande och systematiskt arbete har genomförts, både när det gäller att informationsklassa nya tillgångar och att uppdatera befintliga klassningar.

Förteckningen visar även att det fortfarande finns informationstillgångar som ännu inte är fullt dokumenterade i övriga stödsystem. Närmare bestämt finns 28 informationstillgångar som

ännu inte är registrerade i registerförteckningen i Draftit och som därför bör registreras. Vidare finns 15 informationstillgångar som saknar genomförda riskanalyser.

Även dessa siffror skiljer sig från föregående år. Då saknades 16 informationstillgångar i registerförteckningen och 23 informationstillgångar saknade riskanalyser. Att antalet informationstillgångar som ännu inte är registrerade i registerförteckningen har ökat beror på att arbetet med informationsklassning har omfattat fler tillgångar under året, vilket i sin tur har synliggjort ytterligare system och informationstillgångar som behöver dokumenteras.

Sammanfattningsvis visar jämförelsen att stadsdelsförvaltningen har gjort tydliga framsteg i arbetet med informationsklassning, samtidigt som uppföljningen har bidragit till att identifiera kvarstående utvecklingsområden inom dokumentation och registerföring.

Dataskyddsombudets bedömning samt rekommendationer

Dataskyddsombudet bedömer att stadsdelsförvaltningen i huvudsak har en fungerande och ändamålsenlig struktur för dokumentation av personuppgiftsbehandlingar. Registerförteckningen utgör ett centralt verktyg i dataskyddsarbetet och ger i stora delar en god överblick över hur personuppgifter behandlas inom stadsdelsförvaltningen.

Vid granskningen av genomförda informationsklassningar har det dock framkommit att vissa system som innehåller personuppgifter ännu inte har registrerats i registerförteckningen. Avsaknaden av dessa registreringar innebär att registerförteckningen inte är heltäckande, vilket försvårar möjligheten att arbeta fullt ut systematiskt och riskbaserat med dataskydd, i enlighet med dataskyddsförordningens krav.

Mot denna bakgrund rekommenderar dataskyddsombudet att stadsdelsnämnden ger avdelningscheferna på samtliga avdelningar i uppdrag att säkerställa att de system som ännu inte har förts in i registerförteckningen registreras.

Åtgärden bör genomföras under 2026 och syftar till att säkerställa att stadsdelsförvaltningen har en fullständig och korrekt överblick över samtliga personuppgiftsbehandlingar, samt att dokumentationen uppfyller kraven enligt dataskyddsförordningen.

3. Konsekvensbedömning avseende dataskydd

Bakgrund och syfte

En konsekvensbedömning avseende dataskydd krävs när personuppgiftsansvarig planerar att inleda en personuppgiftsbehandling som innebär hög risk för de registrerade. Huruvida en behandling innebär hög risk eller inte behöver personuppgiftsansvarig avgöra genom att genomföra en så kalladtröskelanalys.

En konsekvensbedömning ska vara genomförd för samtliga behandlingar som innebär hög risk, vilket innebär att personuppgiftsansvarig även behöver kontrollera huruvida denne utför befintliga behandlingar som innebär hög risk. Om högriskbehandlingar utförs för vilka en konsekvensbedömning inte har gjorts, behöver personuppgiftsansvarig genomföra en sådan.

Genom att genomföra en konsekvensbedömning kan personuppgiftsansvarig identifiera risker med en personuppgiftsbehandling, hantera riskerna genom åtgärder och rutiner samt påvisa ansvarsskyldighet. Genom konsekvensbedömningar kan risker identifieras och förebyggas.

Syftet med detta rapporteringsområde är att rapportera huruvida verksamheten har ändamålsenliga rutiner som möjliggör att tröskelanalyser och konsekvensbedömningar genomförs, huruvida sådana genomförs när det krävs samt huruvida personuppgiftsansvarig har genomfört konsekvensbedömningar för de behandlingar som kräver det.

Kontroller och iakttagelser gjord av dataskyddsombudet

Finns det ändamålsenliga rutiner för att vid nya/förändrade personuppgiftsbehandlingar genomföra tröskelanalys?

Ja. Det finns ändamålsenliga och tydligt dokumenterade rutiner för hur tröskelanalyser ska genomföras. Stadsdelsförvaltningen tillhandahåller väl utformade mallar och vägledningar som är publicerade på intranätet, och dessa kompletteras av stadens gemensamma instruktioner och stödmaterial för tröskelanalys. Materialet beskriver när en tröskelanalys ska göras, hur den ska genomföras och vilka uppgifter som behöver dokumenteras. Detta ger verksamheterna ett strukturerat och enhetligt stöd för att bedöma om en behandling kan innebära hög risk och om en konsekvensbedömning (DPIA) behöver genomföras.

Genomförs tröskelanalyser vid nya/förändrade personuppgiftsbehandlingar?

Dataskyddsombudets granskning visar att tröskelanalyser endast genomförs i begränsad utsträckning vid nya eller förändrade personuppgiftsbehandlingar. En tröskelanalys, det vill säga en bedömning av om en viss behandling kan medföra hög risk för de registrerades rättigheter och friheter, ska göras inför alla behandlingar där risken bedöms kunna vara förhöjd. Granskningen indikerar att sådana analyser inte alltid genomförs, trots att de hade varit nödvändiga för att avgöra om en fullständig konsekvensbedömning (DPIA) bör genomföras. Detta innebär att vissa behandlingar som potentiellt utgör hög risk inte föregås av den strukturerade riskbedömning som rutinen kräver.

Finns det en ändamålsenlig mall samt rutiner för genomförande av konsekvensbedömning avseende dataskydd?

Ja. Det finns ändamålsenliga mallar och tydligt beskrivna rutiner för hur konsekvensbedömningar avseende dataskydd (DPIA) ska genomföras. Dessa mallar och rutiner finns publicerade både på stadsdelsförvaltningens egen del av intranätet och på stadens gemensamma intranätssidor, vilket gör dem lätt tillgängliga för samtliga verksamheter.

Materialet anger när en konsekvensbedömning ska göras, vilka moment som ska ingå, hur risker ska identifieras och bedömas samt hur föreslagna skyddsåtgärder ska dokumenteras. Som stöd i arbetet skickar dataskyddsombudet dessutom en årlig påminnelse till verksamheterna om att se över och vid behov uppdatera sina konsekvensbedömningar. Detta bidrar till att konsekvensbedömningarna hålls aktuella och att arbetet med dataskydd bedrivs på ett strukturerat och systematiskt sätt.

Genomförs konsekvensbedömning avseende dataskydd i de fall det krävs?

Dataskyddsombudet konstaterar att konsekvensbedömningar avseende dataskydd (DPIA) ännu inte genomförs i alla de fall där det kan krävas. Även om stadsdelsförvaltningen har en välstrukturerad och omfattande registerförteckning saknas det ofta uppgifter om risknivå för de registrerade behandlingarna. Denna brist gör det svårt att identifiera vilka behandlingar som faktiskt utgör potentiella högriskbehandlingar och därmed också vilka som borde ha föregåtts av en konsekvensbedömning.

Det kan därför fastställas att det finns konsekvensbedömningar som saknas, men det är i dagsläget inte möjligt att avgöra omfattningen eller exakt vilka behandlingar som borde ha genomgått en DPIA. Detta understryker behovet av att komplettera registerförteckningen med korrekta risknivåer för att möjliggöra en mer träffsäker och systematisk uppföljning framöver.

Har personuppgiftsansvarig identifierat samtliga personuppgiftsbehandlingar som kräver att en konsekvensbedömning avseende dataskydd görs samt genomfört detta?

Dataskyddsombudet kan konstatera att personuppgiftsansvarig ännu inte fullt ut har identifierat alla personuppgiftsbehandlingar som kräver en konsekvensbedömning avseende dataskydd (DPIA), och att sådana bedömningar därför inte genomförts i den omfattning som behövs. Samtliga avdelningar hanterar behandlingar som potentiellt kan innebära hög risk för de registrerades rättigheter och friheter, vilket innebär att flera av dem sannolikt borde ha föregåtts av en konsekvensbedömning.

Även om Draftit erbjuder en funktion för att klassificera risknivån (låg/medelhög/hög) används denna funktion endast i mycket begränsad omfattning. Avsaknaden av riskklassificering gör det svårt att identifiera vilka behandlingar som faktiskt uppfyller kriterierna för en DPIA. Detta innebär att stadsdelsförvaltningen inte har en fullständig överblick över vilka behandlingar som kräver en konsekvensbedömning, och därmed inte heller har kunnat säkerställa att nödvändiga DPIA:er genomförs.

Detta visar på ett behov av att stärka arbetet med riskklassificering och systematisk uppföljning för att säkerställa efterlevnad av dataskyddsförordningens krav.

Dataskyddsombudets jämförelse med föregående års resultat

Skiljer sig resultatet åt från föregående år och hur i så fall?

Resultatet skiljer sig inte nämnvärt från föregående år. De brister och risker som identifierades tidigare kvarstår till stor del även i årets granskning, särskilt avseende avsaknaden av riskklassificeringar och det begränsade genomförandet av tröskelanalyser och konsekvensbedömningar. Detta innebär att stadsdelsförvaltningen fortsatt har utmaningar kopplade till att systematiskt identifiera högriskbehandlingar och säkerställa efterlevnad av kraven på DPIA. Samtidigt visar årets resultat att situationen inte har försämrats, utan snarare att samma förbättringsområden alltjämt behöver hanteras.

Dataskyddsombudets bedömning samt rekommendationer

Dataskyddsombudet bedömer att det finns *brister* inom arbetet med konsekvensbedömningar avseende dataskydd. Avsaknaden av genomförda konsekvensbedömningar innebär att vissa behandlingar som potentiellt kan innebära högre risker fortgår utan att verksamheterna har dokumenterat de överväganden och skyddsåtgärder som normalt bör ligga till grund för en sådan behandling. Detta gör att riskerna inte hanteras lika systematiskt som rutinerna avser.

När konsekvensbedömningar inte genomförs i de fall där det är nödvändigt uppfylls inte fullt ut kraven i artikel 35 i dataskyddsförordningen. Det innebär också att stadsdelsförvaltningen får svårare att visa hur man säkerställer lämpliga skyddsåtgärder i enlighet med principen om integritet och konfidentialitet samt ansvarsskyldigheten enligt artikel 32.

Mot denna bakgrund rekommenderar dataskyddsombudet att stadsdelsnämnden ger avdelningscheferna på samtliga avdelningar i uppdrag att under 2026:

- säkerställa att risknivå anges för samtliga behandlingar i Draftit,
- genomföra tröskelanalyser för att identifiera behandlingar som kan innebära hög risk,
- ta fram eller uppdatera konsekvensbedömningar för de behandlingar som bedöms vara högrisk.

Vidare föreslår dataskyddsombudet att nämnden ger dataskyddsombudet i uppdrag att följa upp genomförandet och återrapportera resultatet i årsrapporten för 2026. Detta skapar goda förutsättningar för ett mer strukturerat och komplett arbete med dataskydd framöver.

4. Den registrerades rättigheter

Bakgrund och syfte

Den registrerade har ett antal rättigheter enligt GDPR. Den registrerade kan bland annat begära tillgång (registerutdrag), rättelse eller radering. Den som är personuppgiftsansvarig ska tillmötesgå en begäran enligt de krav som finns.

Syftet med detta rapporteringsområde är att kontrollera huruvida det finns ändamålsenliga mallar samt rutiner för besvarande av rättighetsbegäran, huruvida inkomna begäranden har hanterats inom den tidsram som finns att förhålla sig till samt huruvida svaren till de registrerade, baserat på ett antal stickprov, uppfyller lagkraven.

Kontroller och iakttagelser gjord av dataskyddsombudet

Finns det ändamålsenliga mallar samt rutiner för besvarande av begäran från den registrerade?

Ja. Stadsdelsförvaltningen har ändamålsenliga och väl dokumenterade rutiner för hanteringen av begäranden från registrerade, i enlighet med dataskyddsförordningens krav. Det finns framtagna och lättillgängliga mallar som stödjer verksamheterna i att besvara olika typer av förfrågningar, såsom rätt till tillgång, rättelse, radering, begränsning av behandling och invändningar. Dessa mallar används för att säkerställa att svaren är korrekta, enhetliga och följer gällande regelverk.

Dataskyddsombudet ansvarar för att samordna och kvalitetssäkra hanteringen av begäranden. Inkomna förfrågningar registreras och loggas av dataskyddsombudet, vilket ger en god överblick över antalet ärenden, vilken typ av rättighet som åberopats och hur ärendena har hanterats. Detta bidrar även till att säkerställa att svar lämnas inom lagstadgad tidsfrist.

Sammanfattningsvis finns både strukturerade mallar och tydliga rutiner som stödjer ett rättssäkert och konsekvent arbete med att besvara registrerades begäranden.

Hur många begäranden (om registerutdrag, begränsning, radering etc.) har under året inkommit från de registrerade?

Det har inkommit 5 stycken.

Hur många av de inkomna begärandena har besvarats av verksamheten inom en månad?

Samtliga inkomna begäranden har besvarats inom den lagstadgade tidsfristen om en månad, med undantag för ett ärende. Detta specifika ärende inkom via domstol och krävde därför ytterligare handläggning innan ett korrekt och fullständigt svar kunde lämnas. Fördröjningen var begränsad till endast någon dag utöver den ordinarie tidsfristen. I övrigt har alla begäranden hanterats skyndsamt och inom ramen för dataskyddsförordningens krav.

Baserat på ett antal stickprov genomförda av dataskyddsombudet, uppfyller svaren till de registrerade lagkraven?

Ja. Dataskyddsombudets stickprov visar att de svar som lämnas till de registrerade uppfyller de krav som ställs i dataskyddsförordningen. Stadsdelsförvaltningen använder gemensamma,

standardiserade mallar som tagits fram av dataskyddsombudet, vilket säkerställer att svaren innehåller de uppgifter som krävs och att de är korrekta, tydliga och enhetligt utformade. Mallarna fungerar som ett stöd för verksamheterna och minskar risken för att viktig information utelämnas. Stickproven bekräftar därmed att rutinen fungerar som avsett och att svaren håller en god och rättssäker kvalitet.

Dataskyddsombudets jämförelse med föregående års resultat

Skiljer sig resultatet åt från föregående år och hur i så fall?

Nej, resultatet skiljer sig inte från föregående år. Dataskyddsombudets uppföljning visar att hanteringen av registrerades begäranden fortsatt sker på ett enhetligt och rättssäkert sätt, i samma utsträckning som tidigare. Rutinerna följs, mallarna används och begäranden besvaras inom föreskriven tid, vilket innebär att stadsdelsförvaltningen håller en stabil nivå när det gäller efterlevnad av regelverket. Det har varken identifierats någon försämring eller några större förändringar i årets resultat jämfört med föregående år.

Dataskyddsombudets bedömning samt rekommendationer

Dataskyddsombudet bedömer att stadsdelsförvaltningen har goda förutsättningar för att hantera registrerades rättigheter på ett korrekt och rättssäkert sätt samt inom den tidsfrist som dataskyddsförordningen kräver. De rutiner och mallar som finns på plats fungerar väl och bidrar till en enhetlig och lagenlig hantering av inkomna begäranden.

Vid årets granskning har dataskyddsombudet inte identifierat några nämnvärda brister i processen. Inkomna begäranden registreras, följs upp och besvaras i stort sett alltid inom utsatt tid, och de svar som lämnas håller hög kvalitet. Mot bakgrund av detta finns inga särskilda råd eller rekommendationer till stadsdelsnämnden för detta område i nuläget.

Stadsdelsförvaltningen bedöms således ha en stabil och välfungerande hantering av registrerades rättigheter.

5. Personuppgiftsincidenter

Bakgrund och syfte

Med begreppet personuppgiftsincident avses en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats.

Om en inträffad personuppgiftsincident medför en risk för fysiska personers rättigheter och friheter ska den anmälas till Integritetsskyddsmyndigheten (IMY) inom 72 timmar från upptäckt. Om personuppgiftsincidenten sannolikt leder till hög risk för de registrerade måste de informeras utan onödigt dröjsmål.

Om en personuppgiftsincident inte bedöms vara anmälningspliktig ska den dokumenteras.

Syftet med detta rapporteringsområde är att kontrollera huruvida det säkerställs att samtliga medarbetare har den kunskap som krävs om personuppgiftsincidenter, huruvida det finns ändamålsenliga rutiner för att hantera händelser som kan utgöra personuppgiftsincidenter och huruvida dessa rutiner följs.

Kontroller och iakttagelser gjord av dataskyddsombudet

Hur säkerställs det att samtliga medarbetare har den kunskap som behövs för att veta hur denne ska agera vid en personuppgiftsincident?

Stadsdelsförvaltningen säkerställer att medarbetarna har den kunskap som krävs genom flera stödjande strukturer. Det finns tydliga rutiner, vägledningar och instruktionsmaterial publicerade på intranätet som beskriver hur en personuppgiftsincident ska identifieras, rapporteras och hanteras. Informationen omfattar både praktiska steg och ansvarsfördelning, vilket ger medarbetarna ett lättillgängligt stöd vid eventuella incidenter.

Det är den närmaste chefens ansvar att säkerställa att medarbetarna känner till dessa rutiner och förstår hur de ska agera om en incident skulle inträffa. Cheferna förväntas informera nyanställda, följa upp kunskapen vid behov samt ta upp rutinerna i samband med introduktion eller vid förändringar i arbetsprocesser. På så sätt skapas en kontinuerlig medvetenhet och förståelse i organisationen för hur personuppgiftsincidenter ska hanteras på ett korrekt och snabbt sätt.

Finns det ändamålsenliga rutiner för att hantera händelser som kan utgöra potentiella personuppgiftsincidenter? Följs dessa?

Ja. Stadsdelsförvaltningen har ändamålsenliga rutiner för att hantera händelser som kan utgöra potentiella personuppgiftsincidenter. Rutinerna beskriver bland annat hur en incident ska identifieras, vilka uppgifter som ska dokumenteras, vem som ska informeras och hur bedömningen av incidentens allvarlighetsgrad ska göras. De innehåller även stöd för att avgöra när en incident ska anmälas till IMY samt när berörda registrerade ska informeras.

Rutinerna är tillgängliga via intranätet och följs av verksamheterna i den utsträckning incidenter uppstår. Dataskyddsombudet stödjer arbetet vid behov och säkerställer att bedömningar och rapportering görs enligt gällande regelverk. Detta bidrar till att eventuella incidenter hanteras snabbt, korrekt och på ett enhetligt sätt inom stadsdelsförvaltningen.

Hur många personuppgiftsincidenter har dokumenterats under året?

17 stycken personuppgiftsincidenter har dokumenterats under året.

Hur många personuppgiftsincidenter har anmälts till IMY under året?

13 stycken personuppgiftsincidenter har anmälts till IMY under året.

Dataskyddsombudets jämförelse med föregående års resultat

Skiljer sig resultatet åt från föregående år och hur i så fall?

Det är svårt att göra en direkt jämförelse med föregående år eftersom en ny rutin för hantering och anmälan av personuppgiftsincidenter trädde i kraft efter sommaren 2025. Den tidigare rutinen innehöll vissa oklarheter och var inte fullt ut förenlig med dataskyddsombudets roll enligt dataskyddsförordningen. Dessa brister har även identifierats i stadsdelsförvaltningens tidigare GDPR årsrapport och lyfts som ett område som behövde åtgärdas.

I den reviderade rutinen tydliggörs nu att dataskyddsombudet ska ha både en stödjande och en granskande funktion, men att det yttersta ansvaret för efterlevnaden av dataskyddsregelverket ligger hos den personuppgiftsansvariga, det vill säga respektive nämnd eller bolagsstyrelse. Det innebär att verksamheten ansvarar för det praktiska arbetet med att identifiera, bedöma och, när det krävs, anmäla personuppgiftsincidenter till Integritetsskyddsmyndigheten. Detta ska göras i samråd med dataskyddsombudet, som ger vägledning och stöd men inte själv ansvarar för anmälan.

Sammanfattningsvis har den nya rutinen inneburit en tydligare ansvarsfördelning och bättre överensstämmelse med dataskyddsförordningens krav. Därför går årets resultat inte att fullt ut jämföra med föregående års, då förutsättningarna för incidenthanteringen har förändrats.

Dataskyddsombudets bedömning samt rekommendationer

Dataskyddsombudet konstaterar att de incidenter som inte rapporterades inom föreskriven tid huvudsakligen berodde på att dataskyddsombudet inte informerades inom 72 timmar från det att incidenterna upptäcktes. Detta tyder på brister i de organisatoriska rutinerna, framför allt gällande medarbetarnas kunskap om hur och när incidenter ska rapporteras. I flera fall har medarbetare inte varit medvetna om att incidenter ska vidarebefordras omgående.

Den nya rutin som införts innebär att incidenter ska rapporteras till närmaste chef i stället för direkt till dataskyddsombudet. Denna förändring tydliggör chefernas ansvar, men innebär samtidigt en risk för osäkerhet kring om medarbetare kommer att rapportera vidare incidenter i tid eller om information riskerar att fördröjas. Det finns därför fortsatt behov av att stärka kännedomen om rutinen hos samtliga medarbetare.

Vid granskningen har dataskyddsombudet även uppmärksammat att informationen till registrerade vid incidenter som bedömts innebära hög risk fortfarande är otillräcklig. Endast i sex av de aktuella fallen har berörda personer informerats, trots att dataskyddsförordningen kräver att registrerade ska underrättas utan onödigt dröjsmål när en incident kan medföra en hög risk för deras rättigheter och friheter. Detta ställer höga krav på att både rutinen och dess

praktiska tillämpning fungerar väl och säkerställer att information lämnas på ett korrekt, tydligt och skyndsamt sätt i varje sådant fall.

Mot denna bakgrund rekommenderar dataskyddsombudet att stadsdelsnämnden:

- ger verksamheterna i uppdrag att aktivt sprida och förankra rutinen för personuppgiftsincidenter internt,
- säkerställer att medarbetare får tydlig information om sina rapporteringsskyldigheter,
- säkerställer att registrerade informeras vid incidenter som innebär hög risk, i enlighet med dataskyddsförordningens krav.

Dessa åtgärder bedöms vara viktiga för att stärka incidenthanteringen och säkerställa att stadsdelsförvaltningen fullt ut följer regelverket.

6. Överföring till tredje land

Bakgrund och syfte

För att säkerställa att den nivå av skydd för personuppgifter som ställs i GDPR inte undergrävs får överföringar av personuppgifter till länder utanför EU/EES (tredje land) endast ske under särskilda förutsättningar. Det innebär att sådan överföring måste stödjas på antingen ett beslut från EU-kommissionen om att landet ifråga upprätthåller en adekvat skyddsnivå, att överföringen omfattas av en lämplig skyddsåtgärd eller i särskilda undantagsfall. Vidare behöver även kompletterade skyddsåtgärder, utöver de lämpliga skyddsåtgärderna, vidtas i vissa fall.

Syftet med detta rapporteringsområde är att rapportera huruvida personuppgiftsansvarig har identifierat de tredjelandsöverföringar som utförs, huruvida personuppgiftsansvarig tillämpar överföringsverktyg på de tredjelandsöverföringar som utförs och om nödvändiga bedömningar har gjorts avseende tredjelandsöverföringarna.

Kontroller och iakttagelser gjord av dataskyddsombudet

Har personuppgiftsansvarig identifierat de tredjelandsöverföringar som utförs?

Ja. Vid dataskyddsombudets genomgång av stadsdelsförvaltningens registerförteckning, personuppgiftsbiträdesavtal, genomförda konsekvensbedömningar samt påbörjade och avslutade informationsklassningar kan det konstateras att stadsdelsförvaltningen har identifierat och dokumenterat de tredjelandsöverföringar som förekommer.

Den tredjelandsöverföring som har identifierats är kopplad till användningen av Zoom X, ett system som är upphandlat centralt av staden. Överföringen har dokumenterats i registerförteckningen och hanteras i enlighet med stadens gemensamma riktlinjer, avtal och bedömningar för tredjelandsöverföringar.

Under slutet av året har Zoom X ersatts av Nordic for Zoom, vilket bedöms vara ett säkrare alternativ där servrarna är placerade i Sverige. Mot denna bakgrund bedöms det inte längre förekomma någon tredjelandsöverföring kopplad till denna tjänst.

Sammanfattningsvis kan konstateras att stadsdelsförvaltningen har identifierat och dokumenterat de tredjelandsöverföringar som har förekommit samt vidtagit åtgärder som minskar behovet av överföring av personuppgifter till tredje land.

Tillämpar personuppgiftsansvarig ett överföringsverktyg på de tredjelandsöverföringar som utförs?

Stadsdelsförvaltningen tillämpar i nuläget inget eget överföringsverktyg för tredjelandsöverföringar. Den enda identifierade tredjelandsöverföringen har varit kopplad till användningen av Zoom X, ett system som är upphandlat på central nivå inom staden. I och med den centrala upphandlingen hanteras val av överföringsverktyg, avtalsvillkor samt eventuella kompletterande skyddsåtgärder inom ramen för stadens gemensamma avtal och riktlinjer.

Detta innebär att bedömningen av vilka överföringsmekanismer som används, exempelvis standardavtalsklausuler eller andra godkända skyddsåtgärder enligt dataskyddsförordningen,

görs på stadsnivå och inte av stadsdelsförvaltningen. Stadsdelsförvaltningen tillämpar därför inget eget överföringsverktyg, utan följer de säkerhetsåtgärder och bedömningar som fastställts genom stadens centrala upphandling och styrdokument.

Har nödvändig bedömning, ”Transfer Impact Assessment” (TIA), gjorts avseende tredjelandsöverföringarna?

Ja. En nödvändig bedömning, så kallad Transfer Impact Assessment (TIA), har genomförts på central nivå inom staden. Denna stadsinterna TIA har omfattat de tredjelandsöverföringar som varit kopplade till användningen av Zoom X och har legat till grund för stadens bedömning av risker samt beslut om vilka skyddsåtgärder som ska tillämpas.

Under året har Zoom X ersatts av Nordic for Zoom. I nuläget har stadsdelsförvaltningen dock inte fått ta del av någon uppdaterad eller ny TIA som specifikt avser Nordic for Zoom. Detta innebär att stadsdelsförvaltningen inte fullt ut kan verifiera om och i vilken omfattning eventuella tredjelandsöverföringar förekommer i samband med användningen av den nya tjänsten.

Eftersom systemet är upphandlat och hanteras centralt ansvarar staden för att genomföra och vid behov uppdatera TIA:n. Stadsdelsförvaltningen följer de riktlinjer och bedömningar som fastställs på central nivå och är beroende av att sådana analyser tillhandahålls för att kunna säkerställa full efterlevnad.

Dataskyddsombudets jämförelse med föregående års resultat

Skiljer sig resultatet åt från föregående år och hur i så fall?

Det går inte att göra en direkt jämförelse med föregående år. Dels har årets mall för uppföljning och rapportering förändrats jämfört med tidigare år, vilket innebär att frågorna inte fullt ut motsvarar de som använts tidigare. Dels rör den identifierade tredjelandsöverföringen ett system som är upphandlat och hanterat på central nivå inom staden.

Eftersom bedömningar och skyddsåtgärder, inklusive TIA, genomförs centralt och inte av stadsdelsförvaltningen själv, skiljer sig förutsättningarna från tidigare uppföljningar. Detta innebär att resultatet inte är direkt jämförbart med tidigare års granskningar.

Dataskyddsombudets bedömning samt rekommendationer

Dataskyddsombudet bedömer att det i nuläget finns begränsade möjligheter att dra ytterligare slutsatser på förvaltningsnivå avseende tredjelandsöverföringar, eftersom systemet Zoom X har varit upphandlat och hanterats centralt av staden. Ansvar för bedömningar, val av överföringsverktyg samt genomförande och uppdatering av nödvändiga Transfer Impact Assessments (TIA) ligger på stadsövergripande nivå. Detta innebär att stadsdelsförvaltningen inte själv har möjlighet att påverka eller genomföra kompletterande utredningar inom dessa delar.

Inom ramen för sitt eget ansvar kan stadsdelsförvaltningen däremot, vid framtida upphandlingar och inköp av system, arbeta aktivt för att i möjligaste mån undvika tredjelandsöverföringar. Detta kan exempelvis ske genom att ställa krav på att personuppgifter lagras och behandlas inom EU/EES eller att leverantörer kan visa på adekvata skyddsåtgärder som eliminerar behovet av överföring till tredje land.

Mot denna bakgrund finns det i nuläget inga ytterligare rekommendationer till stadsdelsnämnden kopplade till den centralt upphandlade tjänsten. Det är dock fortsatt viktigt att stadsdelsförvaltningen beaktar frågor om tredjelandsöverföringar vid framtida systemval och egna upphandlingar för att säkerställa ett högt skydd för personuppgifter.

Bilaga 2 – Andra genomförda granskningar och omvärldsbevakning

Andra granskningar som dataskyddsombudet har genomfört under året

Uppföljning av personuppgiftsbiträdesavtal

I föregående års årsrapport uppmärksammade dataskyddsombudet att verksamheterna i flera fall inte hade kopplat sina personuppgiftsbiträdesavtal till de tillhörande huvudavtalen. Ett personuppgiftsbiträdesavtal ska alltid knytas till ett huvudavtal, och bristen på sådan koppling, samt avsaknaden av diarieföring som bilagor till huvudavtalen, innebar att dokumentationen inte var fullständig eller tillräckligt spårbar.

Under det senaste året har stadsdelsförvaltningen vidtagit åtgärder för att stärka detta arbete. Rutinen för hantering av personuppgiftsbiträdesavtal har uppdaterats och formellt fastställts, vilket skapat ett tydligare ramverk för hur avtalen ska tas fram, kopplas samman och diarieföras. Arbetssättet med att systematiskt koppla personuppgiftsbiträdesavtalen till huvudavtalen har också implementerats i verksamheterna.

Dataskyddsombudet bedömer att dessa förbättringar har haft en positiv effekt och att arbetet med personuppgiftsbiträdesavtal har utvecklats i rätt riktning. Det är dock viktigt att det fortsatta arbetet upprätthålls och följs upp så att rutinerna tillämpas konsekvent i samtliga verksamheter.

Dataskyddsombudets rekommendationer baserat på iakttagelserna ovan

Dataskyddsombudets rekommendationer
Dataskyddsombudet rekommenderar att stadsdelsnämnden ger verksamheterna i uppdrag att fortsätta koppla sina personuppgiftsbiträdesavtal till huvudavtal och diarieför dem som bilaga till huvudavtalet.

Omvärldsbevakning

Resultatet av dataskyddsombudets omvärldsbevakning

Dataskyddsombudet har under året genomfört omvärldsbevakning genom Integritetsskyddsmyndighetens (IMY) nyheter och aktuella utvecklingsområden inom dataskydd. Ett av de mest betydelsefulla initiativen som IMY lyft är det vägledningsprojekt som myndigheten startat tillsammans med socialförvaltningen i Kalmar kommun. Projektet fokuserar på hur socialtjänsten kan använda AI-baserade verktyg på ett säkert, ansvarsfullt och integritetsskyddande sätt.

Syftet med projektet är att undersöka hur AI kan stödja socialtjänsten i det dagliga arbetet, exempelvis genom att spela in, transkribera och sammanfatta samtal med klienter. Genom att automatisera delar av den administrativa dokumentationen kan socialsekreterare frigöra tid, vilket i sin tur kan bidra till ökad kvalitet och stärkt professionellt bemötande i mötet med barn, unga och vuxna som behöver stöd.

Resultaten från projektet förväntas fungera som vägledning även för andra kommuner och socialtjänster i landet, och utgöra ett viktigt underlag för hur AI kan införas och användas på ett säkert sätt inom välfärdssektorn. Dataskyddsombudet följer utvecklingen noggrant för att kunna omsätta relevanta lärdomar i stadsdelsförvaltningens fortsatta dataskyddsarbete.

Dataskyddsombudet har även granskat de nya reglerna om kamerabevakning som började gälla den 1 april 2025 och som innebär flera betydande förändringar för verksamheter inom kommunen.

De nya bestämmelserna innebär i korthet följande:

- **Tillståndsplikt hos Integritetsskyddsmyndigheten (IMY) har avskaffats.** Ingen verksamhet behöver längre ansöka om tillstånd för kamerabevakning hos IMY.
- **Eget ansvar för intresseavvägning.** De verksamheter som tidigare var tillståndspliktiga ska nu själva genomföra och dokumentera en intresseavvägning mellan behovet av bevakning och den enskildes rätt till personlig integritet. Bevakning får endast ske om bevakningsintresset väger tyngre.
- **Krav på dokumentation och förteckning.** Verksamheter ska föra en förteckning över den kamerabevakning som bedrivs och även över bevakning som har upphört under de senaste fem åren.
- **Utökade möjligheter för brottsbekämpande myndigheter.** Polisen och andra brottsbekämpande aktörer får ökade möjligheter att använda kamerabevakning i sin operativa verksamhet.

Det är viktigt att notera att själva **principerna för intresseavvägningen inte har förändrats**. Bedömningen ska även fortsättningsvis göras med samma noggrannhet och med integritetsskyddet som utgångspunkt. Skillnaden är att IMY inte längre prövar och godkänner bevakningen i förväg. Det är nu den ansvariga myndigheten, kommunen eller annan aktör med uppgift av allmänt intresse som själv ska säkerställa att bevakningen är tillåten.

IMY:s vägledningar för intresseavvägning vid kamerabevakning finns fortfarande tillgängliga och kan användas som stöd i arbetet. Dataskyddsombudet följer utvecklingen och stödjer

verksamheterna i att anpassa sig till de nya reglerna och säkerställa att dokumentation och bedömningar görs på ett korrekt sätt.

Övrigt att rapportera

Dataskyddsombudet har inga ytterligare iakttagelser eller frågor att rapportera inom ramen för årets GDPR-uppföljning. Samtliga relevanta områden har behandlats i rapporten, och det finns inga ytterligare avvikelser, observationer eller behov av åtgärder att lyfta utöver det som redan redovisats.